

# 7 Data Protection Principles You Need To Follow

“Internet users generate about 2.5 quintillion bytes of data each day”, as per TechJury (Source 1). And, this customer information is most valuable as it ultimately leads to [audience monetization](#). Hence, as a data-driven business, it's your responsibility to adhere to the data protection principles provided by GDPR.

Since most businesses are looking forward to [people-based marketing](#), it becomes even more important for you to secure your customer data. These GDPR principles help a great deal in processing your data.



So moving on, let's understand more about data protection and data protection principles?

## What is Data Protection?

Data protection deals with the storage, usage and process customer information from any external or internal threats, data loss or data corruption. As every audience data you have is personal information of every individual, it's crucial to protect the data.

Hence, many privacy policies such as GDPR, Data Protection Act UK, CCPA and more were formed to secure customer information from illegal use.

It also helps the customers to have complete control of the way their personal information gets used for any marketing purposes. Therefore, GDPR and ePrivacy directive data protection principles came into existence.

Now, we'll understand some simple concepts related to data protection laws and then move on to the data protection principles.

## Some Basic Concepts Regarding Data

Before we touch on the data privacy principles, let's brush on a few common concepts.

### Data Processing

Any activity you do which involves data, i.e., data collection, storing, segmenting the data, deriving insights, leveraging it for marketing efforts, and even erasing the data is together known as data processing.

### Data Controller

Any organization or an individual marketer who deals with customer data for business purposes is known as a data controller. The data controller should adhere to data protection principles while processing the data.

### Privacy by Design and Default

It refers to the way you protect your customer identities while you leverage it in your business efforts. Most importantly, data privacy deals with safeguarding the PII of your customer data.

It deals with the measures you take to protect your data from any cyberattacks or data breach. Any lapse in [data security](#) measures can lead to heavy losses for your business. Hence, many companies heavily invest in data security measures.

So all these concepts mentioned above really help in understanding data protection principles.

## A Brief About GDPR

The GDPR (The General Data Protection Regulation) is the data protection and privacy law created by and for the usage of the EU (European Union) and EEA (European Economic Area). It deals with the protection of personal data and also the transfer of data outside the EU or EEA.

Any businesses who deal with data should [adhere to the GDPR guidelines](#) and also any local privacy policies (if any). Since data is the personal information of individuals, companies need to take necessary measures to protect it from any cyber attacks, corruption or theft.

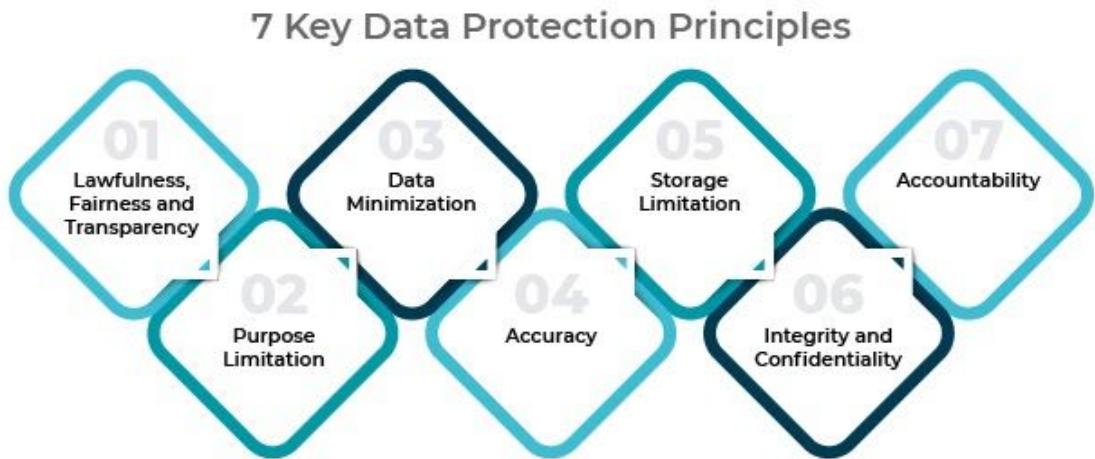
Of course, GDPR is not the only body for governing data protection and privacy. There are many others like the Data Protection Act by the UK (an extension of GDPR and implemented as per UK rules), CCPA, and more.

However, if you deal with a global audience, then you need to be compliant with GDPR and along with any other regulations put forth by the respective Supervisory Authority. All these guidelines ensure that your customer data (identity) is safe and is not used illegally for business purposes.

So, on these lines, GDPR has various policies and once among them is the data protection principles given in Article 5 of GDPR.

Furthermore, let's see what the principles of data protection are and how it impacts your businesses.

## 7 Data Protection Principles by GDPR



## Lawfulness, Fairness and Transparency

This data protection principle indicates that you should process any data lawfully, fairly and transparently. Meaning, your customers should be aware of how their information is utilized or whether you use it in a privacy-safe way.

## Purpose Limitation

As per data protection principles, you should gather or leverage personal data for specific purposes. And should use it legitimately and explicitly for that specified purpose only.

## Data Minimization

As per [data lifecycle](#), your customer data changes, and it becomes irrelevant after a point. Hence, you can't store the same data for a large amount of time.

As per the data minimization principle, you should store the data which is relevant and limit it to your current purpose. You need to delete the excess data from time to time. Indeed, it's one of the crucial data protection principles that can save you a lot of expenses.

# Accuracy

Maintaining accurate data not only helps your business growth but also crucial as per data protection law. As per this GDPR principle, you should maintain accuracy in data which you process and only data that is relevant to your purpose should be stored.

# Storage Limitation

It is one of the data protection principles which states that you should accumulate only the required personal data. You should remove any extra information from the database. Limited data storage will help you maintain data accuracy and remain compliant with data privacy policies.

# Integrity and Confidentiality

Your customer data is a valuable asset for your business. So, it's continuously under several threats that put your customers' privacy at risk. Hence, maintaining the confidentiality and integrity of your data is quite essential.

This GDPR data protection principle indicates the importance of data security measures. And its role in safeguarding your data from unauthorized access, threat and loss of data.

# Accountability

As a data controller, you are accountable for the data which you process. According to this principle of data protection, controllers should demonstrate that they are responsible for the information which they collect. And showcase compliance in the form of records or implemented processes.

# Is DigitalKites Compliant With All 7 Data Protection Principles?

Of course, Digitalkites is an open, collaborative platform which adheres to data privacy policies while dealing with data. You can leverage your data for various [marketing and advertising](#) purposes through DigitalKites in a completely protected environment.

[DigitalKites](#) is an ISO 27001 certified company that takes all the required measures while you leverage it for marketing efforts.

From implementing a consent management platform to leveraging the anonymized data, DigitalKites ensures that you can use your data in a secured manner.

Please contact us to know more about DigitalKites and a wide range of features like audience segmentation, [data onboarding](#), identity resolution, etc.

## Conclusion

These seven fundamental principles of data protection are general in nature but are relevant to every business which deals with data. Any misuse or data theft while processing data will lead to unforeseen consequences and result in a huge loss for your business.

And, not following these data protection principles may land you in the soup as GDPR, CCPA, or any other policies are quite stringent. Hence, implementing data security measures such as anonymization hashing, encryption and so on makes you compliant with the core principles of GDPR.

Especially in the [Madtech space](#) where you specifically deal with customer data, it becomes essential to follow the data protection principles under GDPR.